Commentaire sur la loi sur le renseignement

verfassungsblog.de/commentaire-sur-la-loi-sur-le-renseignement/

Julia Schmitz Do 2 Jul 2015

La nouvelle loi sur le renseignement devait assurer le difficile équilibre entre la transparence démocratique et le secret-défense, l'efficacité de la sécurité et la garantie des libertés, la nécessité de la réflexion et celle de l'urgence**.**

L'absence de cadre légal en matière de renseignement rendait urgente l'élaboration d'un texte [1]. Le gouvernement a donc eu recours à la procédure accélérée pour l'adoption de son projet de loi déposé en mars 2015. Le texte a pourtant fait l'objet de nombreux amendements, témoignant de l'ampleur des problématiques soulevées, au moment même où le Sénat américain vient de réduire les pouvoirs de la NSA.

La loi entend garantir le respect de la vie privée dans toutes ses composantes (données personnelles, secret des correspondances, inviolabilité du domicile) en légalisant les techniques de renseignement[2] tout en renforçant le rôle des agents (anonymat, protection pénale, garantie des sources d'informations). Le "cahier des charges" de la légalité des opérations de renseignement est ainsi précisé : compétence de l'autorité, régularité de la procédure, conformité aux missions, justification et proportionnalité. Le texte précise également que les avocats, les journalistes, les parlementaires ou les magistrats ne peuvent faire l'objet d'une mesure de surveillance au titre de leur fonction[3] et assure une protection des lanceurs d'alerte[4].

Mais la loi est cependant susceptible de porter atteinte aux libertés individuelles et risque la censure du Conseil constitutionnel sur plusieurs points.

Les nouvelles dispositions procèdent en premier lieu à une **extension des finalités et du périmètre de l'activité de renseignement.**

Il est précisé que la politique publique de renseignement relève exclusivement de la compétence de l'Etat afin d'écarter toute privatisation de ce secteur en raison du rôle d'intermédiaire joué par les opérateurs de réseaux, et qu'elle concourt à la défense des intérêts fondamentaux de la Nation ainsi qu'à leur « promotion »[5]. Ses finalités ont été élargies, dépassant le cadre du terrorisme, pour y inclure « l'indépendance nationale, l'intégrité du territoire et la défense nationale », les « intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux et la prévention de toute forme d'ingérence étrangère », les « intérêts économiques, industriels et scientifiques majeurs de la France », la « prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous, des violences collectives de nature à porter atteinte à la paix publique », de « la criminalité et de la délinquance organisées » et de « la prolifération des armes de destruction massive »[6]. Ces finalités semblent sujettes à une interprétation extensive, susceptible de viser certains mouvements sociaux, syndicaux ou politiques.

La Communauté du renseignement comprend un second cercle de services non spécialisés, relevant des Ministres de la défense, de l'intérieur, de l'économie, du budget ou des douanes[7]. En raison de la problématique du renseignement pénitentiaire, le ministère de la justice a finalement été exclu de ce périmètre.

Le flou de certaines dispositions peut constituer une incompétence négative du législateur. Ainsi, les modalités de mise en œuvre des mesures de surveillance internationales sont renvoyées à un décret en Conseil d'Etat non publié[8].

Certains dispositifs permettant de générer une surveillance non pas ciblée mais « indiscriminée » peuvent porter atteinte au **principe de proportionnalité**, pourtant énoncé comme principe directeur.

Il est ainsi prévu d'étendre les interceptions de sécurité aux personnes appartenant à l'entourage de la personne visée, susceptibles de fournir des informations, et de recueillir les données de connexion des téléphones portables par un « dispositif technique de proximité ». En matière de prévention du terrorisme, le texte permet

également d'obliger les opérateurs de réseaux à détecter une succession suspecte de données de connexion par le moyen d'algorithmes, garantissant faiblement l'anonymat des métadonnées recueillies. Or la distinction entre données et contenus de données est aujourd'hui problématique car le seul accès aux données de connexion par ces logiciels espions peut constituer une ingérence considérable dans la vie privée.

En matière de lutte contre le financement du terrorisme, la cellule de renseignement financier peut demander à toute entreprise de transport et à tout opérateur de voyage les éléments d'identification et de parcours des personnes ayant bénéficié d'une prestation, sans autre précision[9]. Les entreprises de transport public routier international de voyageurs ont également l'obligation de recueillir l'identité des passagers[10].

Si des garanties supplémentaires sont prévues dans le respect du principe de subsidiarité (limitation du recours à la procédure d'urgence, réduction de la durée d'autorisation, définition stricte des services habilités), des **techniques plus intrusives** sont légalisées : captation à distance de conversations ou de données informatiques, géolocalisation d'une personne, d'un véhicule ou d'un objet, sonorisation ou captation d'images et de données informatiques pouvant nécessiter l'introduction dans un véhicule, un lieu privé ou un système informatique.

Le texte procède également à un **allongement des délais de conservation** des données, dont le point de départ est toutefois calculé à compter de leur recueil et non de leur exploitation. Concernant les interceptions de sécurité, il passe de 10 à 30 jours. Il est fixé à 120 jours pour les données recueillies par la sonorisation des lieux et véhicules et la captation d'images et de données informatiques. Les données de connexion sont quant à elles conservées 4 ans. Pour les données chiffrées, le délai court à compter de leur déchiffrement, avec une durée maximale de 6 ans à partir de leur recueil, mais un délai de conservation indéfini est prévu pour les données nécessaires aux besoins de l'analyse technique[11].

En ce qui concerne le dispositif de contrôle des opérations de surveillance placées sous l'autorité du Premier Ministre, est créée une nouvelle Autorité administrative indépendante, la Commission Nationale de contrôle des techniques de renseignement (CNCTR), dotée de pouvoirs plus étendus que l'actuelle Commission nationale de contrôle des interceptions de sécurité. Elle est composée de 9 membres nommés pour 6 ans, dont 2 députés et 2 sénateurs, 2 conseillers d'Etat, 2 magistrats de la cour de Cassation et une personnalité qualifiée. Son président est nommé par le président de la République parmi les membres magistrats, après l'avis des commissions permanentes intéressées des deux assemblées (proposition de loi organique adoptée le 24 juin 2015).

Son pouvoir de recommandation est renforcé (avis, observations et rapport annuel d'activité soumis toutefois au secret défense), son **pouvoir de contrôle amélioré** (accès « permanent, complet et direct » aux registres, renseignements collectés, transcriptions, dispositifs de traçabilité et aux locaux de centralisation des renseignements, information facilitée et garantie, pouvoir de vérification) et sa **saisine étendue** (auto-saisine, saisine par toute personne)[12].

Cependant, **le contrôle exercé *a priori*** semble lacunaire. Excepté les procédés d'identification des données de connexion et d'introduction dans un lieu privé, qui doivent recueillir l'avis direct ou exprès de la CNCTR, les demandes écrites et motivées de recours à une technique de renseignement sont adressées au Premier ministre, qui donne son autorisation pour une durée de 4 mois, après avoir recueilli l'avis du président[13] de la CNCTR. Mais cet avis demeure facultatif. Le Premier Ministre peut passer outre un avis défavorable à condition de motiver sa décision, et si l'avis n'est pas délivré dans le délai de 24 heures, il est réputé rendu. En cas d'urgence absolue, l'autorisation peut même être délivrée sans avis préalable, et en cas de menace imminente, le recours aux interceptions de sécurité ou aux dispositifs de géolocalisation ne nécessite aucune autorisation préalable[14].

Ses pouvoirs semblent également insuffisants. En cas d'irrégularité, elle peut seulement adresser « une recommandation » au Premier Ministre pour interrompre le dispositif. Ce n'est que si celui-ci n'y satisfait pas que son Président peut saisir le Conseil d'Etat[15].

Un nouveau recours juridictionnel est en effet créé devant une formation spécialisée du Conseil d'Etat, ou devant une formation restreinte de l'assemblée plénière ou de la section du contentieux, dont les membres sont

habilités ès qualités au secret de la défense nationale. Ces formations pourront juger, en premier et dernier ressort, des requêtes concernant la mise en oeuvre des techniques de renseignement, et en cas d'illégalité, prononcer l'annulation de l'autorisation, ordonner la destruction des renseignements collectés et condamner l'Etat à indemniser le préjudice subi[16]. Elles peuvent également être saisies des requêtes concernant les fichiers intéressant la sûreté de l'État[17].

La saisine est ouverte à la CNCTR, à tout juge dans le cadre d'un litige relatif à une technique de renseignement et à toute personne ayant préalablement saisi la CNCTR. Ce recours est automatique et suspensif en cas d'autorisation délivrée après avis défavorable permettant l'introduction dans un lieu privé[18].

Les nécessités du secret défense interfèrent néanmoins sur les garanties procédurales : les exigences du contradictoire (actes non communiqués, audition séparée des parties), le principe de motivation des décisions (élément protégés par le secret défense), ainsi que la publicité des audiences sont ainsi adaptés[19].

Si les pouvoirs de contrôle de la **délégation parlementaire au renseignement** ont été renforcés, l'on peut noter l'absence de la **Commission nationale de l'informatique et des libertés** puisque les fichiers de données de connexion sont aujourd'hui exclus de son périmètre d'action. Il est pourtant prévu que les agents du renseignement puissent avoir accès aux fichiers relatifs aux infractions pénales[20]. Elle sera seulement consultée pour avis sur les modalités de mise en œuvre des accès aux données de connexion et du nouveau fichier judiciaire national automatisé des auteurs d'infractions terroristes[21].

Si l'accès aux données de connexion a fait l'objet d'une condamnation de la Cour de Justice de l'Union Européenne[22] et d'une procédure pendante devant le Conseil constitutionnel, saisi d'une question prioritaire de constitutionnalité relative à la loi de programmation militaire du 18 décembre 2013[23], la nouvelle loi sur le renseignement doit faire l'objet d'un contrôle *a priori*. Le Conseil a en effet été saisi le 25 juin 2015 et doit rendre sa décision dans un mois.

[1] J.-J. Urvoas et P. Verchère, Rapport d'information n° 1022 sur l'évaluation du cadre juridique applicable aux services de renseignement, 2013 ; J.-J. Urvoas, Rapport n° 201 relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2014.

[2] Les techniques de renseignement sont ainsi listées dans le livre VIII du Code de la Sécurité Intérieure et concernent : l'accès aux données de connexion (art L. 851-1 à 7 CSI), les interceptions de sécurité (art L 852-1 CSI), la sonorisation de certains lieux et véhicules et la captation d'images et de données informatiques (L 853-1 à 3 CSI).

[3] Art L 821-5-2 CSI.

[4] Art L 861-3 CSI.

[5] Art L 811-1 CSI.

[6] Art L 811-3 CSI.

[7] Art. L 811-4 CSI.

[8] Art L. 854-1 CSI.

[9] Art L 561-26 du code monétaire et financier.

[10] Art L. 1631-4 du code des transports.

[11] Art. L 822-2 CSI.

[12] Art L 833-1 à 5 CSI.

[13] En cas de question nouvelle ou sérieuse, la formation restreinte ou plénière de la CNTR doit rendre un avis dans les 72 heures.

[14] Art L 821-1 et 6 CSI.

[15] Celui-ci peut toutefois être également saisi par 3 de ses membres, Art. L. 833-6 à 8 CSI. Si elle estime qu'une illégalité est susceptible de constituer une infraction, la CNCTR peut également saisir le procureur de la République, mais elle doit alors demander à la Commission consultative du secret de la défense nationale un avis sur la possibilité de déclassifier les éléments de l'affaire, Art. L 853-3 I al 2 CSI.

[16] Pour l'examen d'une question de droit, l'assemblée du contentieux ou la section du contentieux dans leur formation de droit commun sont compétentes, Art L. 773-7 du code de justice administrative.

[17] Art L 841-1 et 2 CSI.

[18] Art L 853-3 CSI.

[19] Art L 773-3 à 8 du code de la justice administrative.

[20] Art L 234-4 CSI.

[21] Art L 706-25-3 à 14 du code de procédure pénale.

[22] CJUE, 8 avril 2014, Digital Rights Ireland Ltd, n° C-293-12.

[23] CE, 5 juin 2015, *Association French Data Network (Réseau Français de Données) et autres* , N° 388134. Sont visés les articles L. 246-1 à L. 246-5 CSI qui prévoient la possibilité de recueillir des informations et des documents sur sollicitation des opérateurs de réseaux, à des fins de sécurité nationale.

SUGGESTED CITATION Schmitz, Julia: *Commentaire sur la loi sur le renseignement, VerfBlog,* 2015/7/02, http://verfassungsblog.de/commentaire-sur-la-loi-sur-le-renseignement/.